Full Abstraction for Non-Deterministic and Probabilistic Extensions of PCF

Jean Goubault-Larrecq



PLC Festschrift - Sep. 2013

Outline



- 2 PCF(*S*)
 - Syntax
 - Operational Semantics
 - Denotational Semantics
- 3 The Full Abstraction Problem
 - Full Abstraction
 - Definability
 - Full Abstraction in Angelic Cases

4 Conclusion

- Introduction

Outline

1 Introduction

- 2 PCF(*S*)
 - Syntax
 - Operational Semantics
 - Denotational Semantics
- 3 The Full Abstraction Problem
 - Full Abstraction
 - Definability
 - Full Abstraction in Angelic Cases

4 Conclusion

- Introduction

PCF, Full Abstraction

PCF [Plotkin77]:

a call-by-name, simply-typed, higher-order functional language

- no side-effects
- has computational adequacy
- fails full abstraction... except with additional por

-Introduction

PCF, Full Abstraction

PCF [Plotkin77]:

a call-by-name, simply-typed, higher-order functional language

- no side-effects
- has computational adequacy
- fails full abstraction... except with additional por

Here, PCF plus specific choice effects:

- Will concentrate on angelic non-deterministic choice
- also probabilistic choice, + mixed

└_PCF(*S*)

Outline



- 2 PCF(*S*)
 - Syntax
 - Operational Semantics
 - Denotational Semantics
- 3 The Full Abstraction Problem
 - Full Abstraction
 - Definability
 - Full Abstraction in Angelic Cases

4 Conclusion

Full Abstraction for PCF with Choice		
-PCF(S)		
└─Syntax		



$$\begin{array}{lll} \gamma & ::= & \operatorname{Nat} \mid {\tt S} & \mbox{Ground types} \\ \sigma, \tau & ::= & \gamma \mid \sigma \rightarrow \tau \mid {\tt T}\tau & \mbox{Types} \end{array}$$

Notes:

- S has only one (non-bottom) value
 - = unit type, termination type

Not required in principle, but practical

 \blacksquare T τ type of processes computing value of type τ

à la [Moggi91]

└─PCF(*S*) └─Syntax

PCF(S) Terms

Language parameterized by set $S \subseteq \{A, D, P\}$

(angelic non-det., demonic non-det., probabilistic choice).

PCF terms

```
(\lambda-calculus + basic arithmetic + ifz + fixpoint Y)
```

At S type:

- for every *M* : Nat, ignore *M* : S
- for all M : S, N : σ , sequencing M; N : σ
- At T*τ* types:
 - for each $M: \tau$, val $M: T\tau$
 - for all $M : \sigma, N : T\tau$, $let x \leftarrow M in N : T\tau$
 - Non-det. choice $\bigcirc : T\tau \to T\tau \to T\tau$
 - Prob. choice $\oplus : T\tau \to T\tau \to T\tau$

└─PCF(S) └─Operational Semantics

Operational Semantics

Use judgments $E \cdot M \downarrow^{may} a$, $a \in \mathbb{Q} \cap [0, 1]$.

"The probability that $E \cdot M$ may terminate is > a"

• Redex discovery/computation rule $C \rightarrow C'$:

Final state val_- $\cdot \underline{\top}$: $val_- \cdot \underline{\top} \downarrow^m a$ $(a \in \mathbb{Q} \cap [0, 1))$

Choice:

 $\frac{E \cdot M \downarrow^{\text{may}} a}{E[_MN] \cdot \oslash \downarrow^{\text{may}} a} \quad \frac{E \cdot N \downarrow^{\text{may}} a}{E[_MN] \cdot \oslash \downarrow^{\text{may}} a} \quad \frac{E \cdot M \downarrow^{\text{may}} a \quad E \cdot N \downarrow^{\text{may}} b}{E[_MN] \cdot \oplus \downarrow^{\text{may}} \frac{1}{2}(a+b)} (\oplus)$

└─PCF(S) └─Operational Semantics

Termination Semantics

Definition

 $\Pr(E \cdot M \downarrow^{\mathsf{may}}) = \sup\{a \in \mathbb{Q} \in [0,1] \mid E \cdot M \downarrow^{\mathsf{may}} a \text{ derivable}\}\$

•
$$\Pr(\operatorname{val}_{-} \cdot \underline{\top} \downarrow^{\mathsf{may}}) = 1$$

 $\mathsf{Pr}(E[-MN] \cdot \oplus \downarrow^{\mathsf{may}}) = \frac{1}{2}(\mathsf{Pr}(E \cdot M \downarrow^{\mathsf{may}}) + \mathsf{Pr}(E \cdot N \downarrow^{\mathsf{may}}))$

• $\Pr(E[-MN] \cdot \otimes \downarrow^{may}) = \max(\Pr(E \cdot M \downarrow^{may}), \Pr(E \cdot N \downarrow^{may}))$

PCF(S)

Denotational Semantics: Previsions

Let $[T\tau]_S$ as spaces of previsions over $[\tau]_S$ [JGL-CSL07]

Definition (Prevision on X)

Let I = [0, 1], as a dcpo. A Scott-continuous functional $F : [X \rightarrow I] \rightarrow I$ is a prevision iff:

•
$$F(ah) = aF(h)$$
 for every $a \in I$

$$F(\frac{a+h}{2}) = \frac{1}{2}(a+F(h))$$
 (total mass = 1)

•
$$F(\frac{h+h'}{2}) \leq \frac{1}{2}(F(h)+F(h'))$$

• $F(h) \in \{0,1\}$ for every $h: X \to \{0,1\}$ (if $\mathbf{P} \notin S$)

Note: by representation theorems [JGL08], match the usual Hoare/Smyth powerdomains, as well as [MOW03, TKP05].

PCF(S)

L Denotational Semantics

Denotational Semantics

$$\begin{split} \llbracket \lambda_X \cdot M \rrbracket_S &= (x \mapsto \llbracket M \rrbracket_S) \qquad \llbracket M N \rrbracket_S(\rho) = \llbracket M \rrbracket_S(\llbracket N \rrbracket_S) \\ \llbracket Y \rrbracket_S &= (f \mapsto \bigcup_{n \in \mathbb{N}} f^n(\bot)) \\ \llbracket \operatorname{val} M : \operatorname{T\sigma} \rrbracket_S &= (h \mapsto h(\llbracket M \rrbracket_S)) \\ \llbracket \operatorname{let} x \leftarrow M \text{ in } N \rrbracket_S &= (h \mapsto \llbracket M \rrbracket_S(x \mapsto \llbracket N \rrbracket_S(h)) \\ \llbracket @ \rrbracket_S &= (F_1, F_2, h \mapsto \max(F_1(h), F_2(h)) \\ \llbracket @ \rrbracket_S &= (F_1, F_2, h \mapsto \frac{1}{2}(F_1(h) + F_2(h))(\text{ if } P \in S) \end{split}$$

(ロ)、(型)、(E)、(E)、 E) の(の)

└─PCF(*S*) └─Denotational Semantics

Soundness

In usual PCF, soundness states that if $M \to^* V$ then $\llbracket M \rrbracket = \llbracket V \rrbracket$.

(日) (日) (日) (日) (日) (日) (日) (日)

Theorem (Soundness)

Let
$$\blacklozenge = \chi_{\{\top\}} : [\![S]\!] \to I \text{ map } \perp \text{ to } 0, \top \text{ to } 1$$

(termination-observing continuation).

• If
$$E \cdot M \downarrow^{may}$$
 a then $\llbracket E[M] \rrbracket_S(\blacklozenge) > a$

Proof: induction.

Corollary

└─ PCF(S) └─ Denotational Semantics

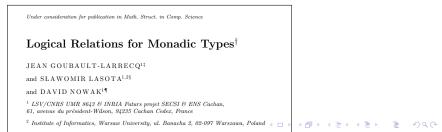
Computational Adequacy

In usual PCF, $M \rightarrow^* V$ iff $\llbracket M \rrbracket = \llbracket V \rrbracket$, at ground types. Here, use $E = _$ (empty context, of type TS \vdash TS)

Theorem (Computational Adequacy)

$$\blacksquare \llbracket M \rrbracket_{\mathcal{S}} (\blacklozenge) = Pr(_\cdot M \downarrow^{\mathsf{may}})$$

Proof: The key point is the definition of a suitable logical relation... and precisely there is a general definition of...



└─ PCF(S) └─ Denotational Semantics

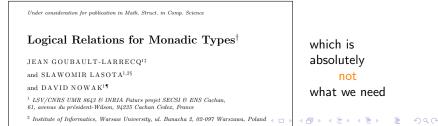
Computational Adequacy

In usual PCF, $M \rightarrow^* V$ iff $\llbracket M \rrbracket = \llbracket V \rrbracket$, at ground types. Here, use $E = _$ (empty context, of type TS \vdash TS)

Theorem (Computational Adequacy)

$$\blacksquare \llbracket M \rrbracket_{\mathcal{S}} (\blacklozenge) = Pr(_\cdot M \downarrow^{\mathsf{may}})$$

Proof: The key point is the definition of a suitable logical relation... and precisely there is a general definition of...



└─PCF(S) └─Denotational Semantics

Computational Adequacy

In usual PCF, $M \rightarrow^* V$ iff $\llbracket M \rrbracket = \llbracket V \rrbracket$, at ground types. Here, use $E = _$ (empty context, of type TS \vdash TS)

Theorem (Computational Adequacy)

$$\blacksquare \llbracket M \rrbracket_{\mathcal{S}} (\blacklozenge) = Pr(_\cdot M \downarrow^{\mathsf{may}})$$

Proof: Define a logical relation R_{σ} by (something like) double orthogonality:

 $M R_{T\sigma} F$ iff for all $E R_{\sigma}^{\perp} h$, $\Pr(E \cdot M \downarrow^{m}) \ge F(h)$

 $E R_{\sigma}^{\perp} h$ iff for all $Q R_{\sigma} v$, $\Pr(E \cdot \operatorname{val} Q \downarrow^m) \ge h(v)$

Then do some stuff and conclude.

- The Full Abstraction Problem

Outline

1 Introduction

- 2 PCF(*S*)
 - Syntax
 - Operational Semantics
 - Denotational Semantics
- 3 The Full Abstraction Problem
 - Full Abstraction
 - Definability
 - Full Abstraction in Angelic Cases

4 Conclusion

└─ The Full Abstraction Problem

Full Abstraction

Full Abstraction

Let $M \preceq^{\text{may}} N$ iff $\Pr(E \cdot M \downarrow^{\text{may}}) \leq \Pr(E \cdot N \downarrow^{\text{may}})$ for every $E : \tau \vdash \text{TS}$.

Conjecture (Full Abstraction)

 $M \preceq^{\text{may}} N \text{ iff } \llbracket M \rrbracket_S \leq \llbracket N \rrbracket_S, \text{ at all types.}$

- Easy direction: If $\llbracket M \rrbracket_S \leq \llbracket N \rrbracket_S$ at type τ , then $\llbracket E[M] \rrbracket_S \leq \llbracket E[N] \rrbracket_S$ for every context $E : \tau \vdash TS$ So $\Pr(E \cdot M \downarrow^{may}) \leq \Pr(E \cdot N \downarrow^{may})$ by computational adequacy.
- Hard direction: assume $\llbracket M \rrbracket_S \leq \llbracket N \rrbracket_S$, find *E* such that $\Pr(E \cdot M \downarrow^{\text{may}}) > \Pr(E \cdot N \downarrow^{\text{may}})$

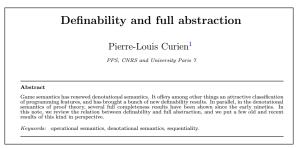
So hard that it is wrong for PCF... but true for PCF(A)!

└─ The Full Abstraction Problem

└─ Definability



Pierre-Louis has always told us that definability was the key to full abstraction.



The Full Abstraction Problem

Definability

Definability...of Opens

So assume $\llbracket M \rrbracket_S \not\leq \llbracket N \rrbracket_S$, of type τ .

■ Since ≤ is specialization ordering of (Scott) topology, there is a separating open set U:

$$\llbracket M \rrbracket_S \in U \qquad \llbracket N \rrbracket_S \notin U$$

• If we can define U by a context E, then:

$$\llbracket E[M] \rrbracket_S = \top \qquad \llbracket E[N] \rrbracket_S = \bot$$

so by computational adequacy

$$\Pr(\operatorname{val} E \cdot M \downarrow^{\mathsf{may}}) = 1 > 0 = \Pr(\operatorname{val} E \cdot N \downarrow^{\mathsf{may}})$$

So $M \not\subset^{\text{may}} N$.

■ By contraposition, $M \preceq^{\text{may}} N$ implies $\llbracket M \rrbracket_S \leq \llbracket N \rrbracket_S$. So full abstraction will hold.

└─ The Full Abstraction Problem

Definability

Definability... of Subbasic Opens

So assume $\llbracket M \rrbracket_S \not\leq \llbracket N \rrbracket_S$, of type τ .

 Since ≤ is specialization ordering of (Scott) topology, there is a separating open set U in a given subbase B_τ:

$$\llbracket M \rrbracket_S \in U \qquad \llbracket N \rrbracket_S \notin U$$

• If we can define U by a context E, then:

$$\llbracket E[M] \rrbracket_S = \top \qquad \llbracket E[N] \rrbracket_S = \bot$$

so by computational adequacy

$$\Pr(\operatorname{val} E \cdot M \downarrow^{\mathsf{may}}) = 1 > 0 = \Pr(\operatorname{val} E \cdot N \downarrow^{\mathsf{may}})$$

So $M \not\subset^{\text{may}} N$.

By contraposition, $M \preceq^{\text{may}} N$ implies $\llbracket M \rrbracket_S \leq \llbracket N \rrbracket_S$. So full abstraction will hold.

└─ The Full Abstraction Problem

Definability

Choosing the Right Subbase

Fortunately:

Lemma

For every type τ , $\llbracket \tau \rrbracket_S$ is a bc-domain.

(One of the nice CCCs of continuous domains.)

Proposition (Key result — coincidence of topologies)

If X and Y are bc-domains, then:

- Scott topology on $[X \rightarrow Y] = pointwise convergence$ Subbasis: $[a \in V] = \{f \mid f(a) \in V\}, a \in X, V \text{ open in } Y$
- Scott topology on previsions on X = weak topology Subbasis: $[h > r] = \{F \mid F(h) > r\}, h \in [X \to I], r \in \mathbb{Q}$

- The Full Abstraction Problem

Definability

Definability of Subbasic Opens

Miracle

All these subbasic opens are definable.

 E.g., on [X → Y], Let a be defined by term t
 Let V be defined by context E
 Then [a ∈ V] is defined by context E[_t].

Mission accomplished!

. . . almost.

We actually need to define elements a as well. Eventually, this requires some additional constructions. E.g., sup of maps requires ∅ (non-det. choice). Worse: prob. choice ⊕ requires statistical termination testers.

└─ The Full Abstraction Problem

Definability

The Purely Angelic Case

Without probabilities, $M \preceq^{may} N$ simplifies to: for every context E, $E \cdot M \downarrow^{may}$ implies $E \cdot N \downarrow^{may}$.

Theorem (Case $S = \{A\}$)

Full abstraction holds for
$$PCF(\{A\})$$
:
 $M \precsim^{may} N \text{ iff } \llbracket M \rrbracket_{\{A\}} \leq \llbracket N \rrbracket_{\{A\}}$

Note 1: No need for parallel or ... which is in fact definable: M por $N = (M || N) \odot (N || M)$ Note 2: Proof much simpler than Plotkin's for PCF+por... but language is different.

Note 3: Implies full abstraction for (isomorphic) semantics using Hoare powerdomains instead of previsions.

└─ The Full Abstraction Problem

Definability

The Angelic+Probabilistic Case

We now need termination testers Pr(M > b) to the language (M : TS)

$$\frac{-\cdot M \downarrow^{\text{may}} b \quad E \cdot \Box \downarrow^{\text{may}} a}{E \cdot \Pr(M > b) \downarrow^{\text{may}} a} (\Pr) \quad \llbracket \Pr(M > b) \rrbracket_{S} = \begin{cases} \top & \text{if } \llbracket M \rrbracket_{S}(\blacklozenge) > b \\ \bot & \text{otherwise} \end{cases}$$

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 のへぐ

- The Full Abstraction Problem

-Full Abstraction in Angelic Cases

The Angelic+Probabilistic Case

Let
$$M \stackrel{\leq m}{\sim} N$$
 iff $\Pr(_\cdot E'[M]\downarrow^m) \le \Pr(_\cdot E'[N]\downarrow^m)$
for every extended context $E' \qquad E' ::= \dots | \Pr(_>b)$

Theorem (Case $S = \{1, P\}$)

 $\begin{aligned} \textit{Full abstraction holds for PCF}(\{\mathtt{A},\mathtt{P}\}) + \textit{statistical testers:} \\ & M \lesssim^{\mathsf{may}} N \textit{ iff } [\![M]\!]_{\{\mathtt{A},\mathtt{P}\}} \leq [\![N]\!]_{\{\mathtt{A},\mathtt{P}\}} \end{aligned}$

Proof. As before, there is a subbasis of definable opens.

- Conclusion

Outline

1 Introduction

- 2 PCF(*S*)
 - Syntax
 - Operational Semantics
 - Denotational Semantics
- 3 The Full Abstraction Problem
 - Full Abstraction
 - Definability
 - Full Abstraction in Angelic Cases

4 Conclusion

Conclusion

Conclusion

The angelic cases ... are angelic:

- PCF({A}) is fully abstract
- PCF({A, P}) is fully abstract

provided we add statistical termination testers

- I cheated a bit: we need a bit of call-by-value to define the probabilistic contexts
- Demonic/erratic cases slightly more difficult
- Purely probabilistic case hopeless

unless we turn to random variables, maybe.